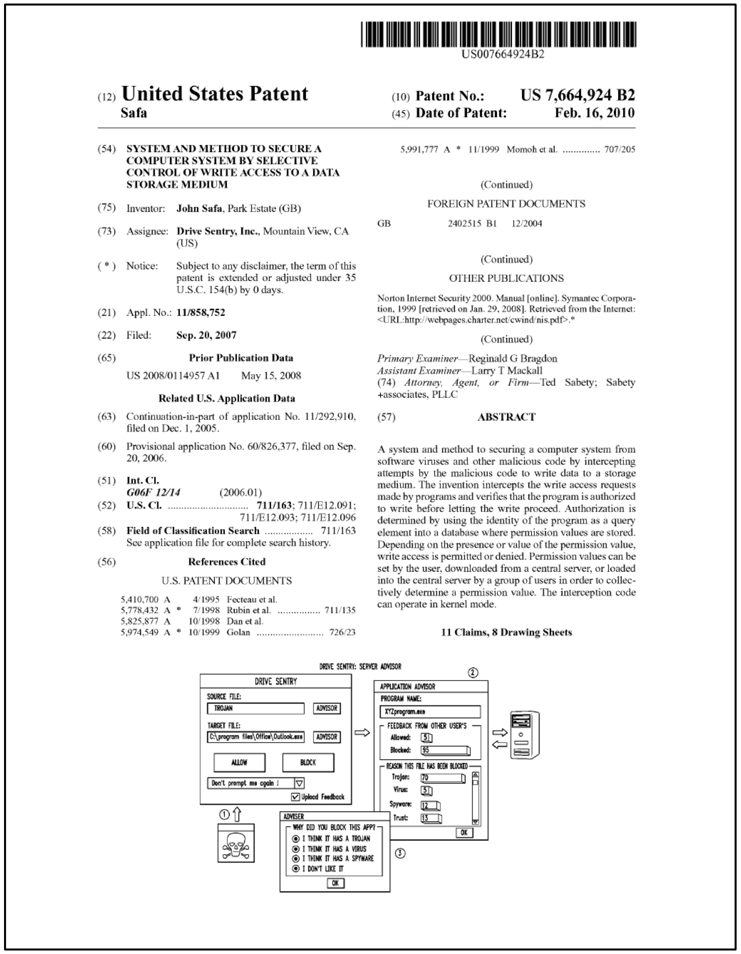
Ex. D - Claim Chart

U.S. Patent No. 7,664,924



US007664924B2

(12) **United States Patent**
Safa

(10) **Patent No.:** **US 7,664,924 B2**
(45) **Date of Patent:** **Feb. 16, 2010**

(54) **SYSTEM AND METHOD TO SECURE A COMPUTER SYSTEM BY SELECTIVE CONTROL OF WRITE ACCESS TO A DATA STORAGE MEDIUM**

(75) Inventor: **John Safa**, Park Estate (GB)

(73) Assignee: **Drive Sentry, Inc.**, Mountain View, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **11/858,752**

(22) Filed: **Sep. 20, 2007**

(65) **Prior Publication Data**

US 2008/0114957 A1 May 15, 2008

Related U.S. Application Data

(63) Continuation-in-part of application No. 11/292,910, filed on Dec. 1, 2005.

(60) Provisional application No. 60/826,377, filed on Sep. 20, 2006.

(51) **Int. Cl.**
G06F 12/14 (2006.01)

(52) **U.S. Cl.** **711/163**; 711/E12.091; 711/E12.093; 711/E12.096

(58) **Field of Classification Search** 711/163
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,410,700	A		4/1995	Fecteau et al.	
5,778,432	A	*	7/1998	Rubin et al.	711/135
5,825,877	A		10/1998	Dan et al.	
5,974,549	A	*	10/1999	Golan	726/23
5,991,777	A	*	11/1999	Momoh et al.	707/205

(Continued)

FOREIGN PATENT DOCUMENTS

GB	2402515 B1	12/2004

(Continued)

OTHER PUBLICATIONS

Norton Internet Security 2000. Manual [online]. Symantec Corporation, 1999 [retrieved on Jan. 29, 2008]. Retrieved from the Internet: <URL:http://webpages.charter.net/cwind/nis.pdf>.*

(Continued)

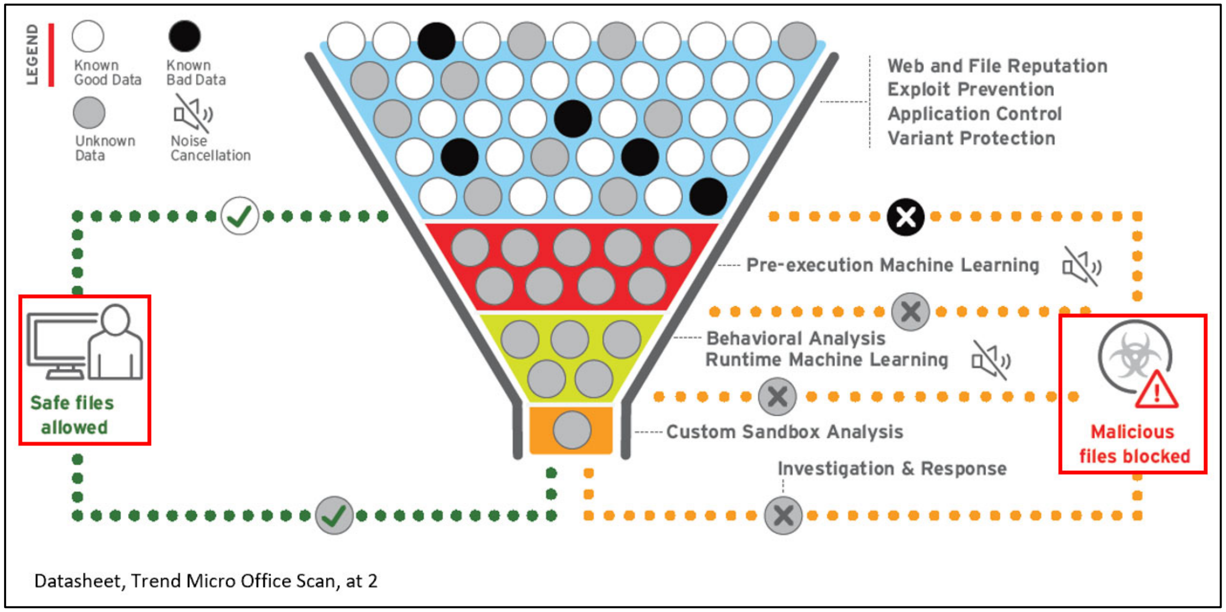
Primary Examiner—Reginald G Bragdon
Assistant Examiner—Larry T Mackall
(74) *Attorney, Agent, or Firm*—Ted Sabety; Sabety +associates, PLLC

(57) **ABSTRACT**

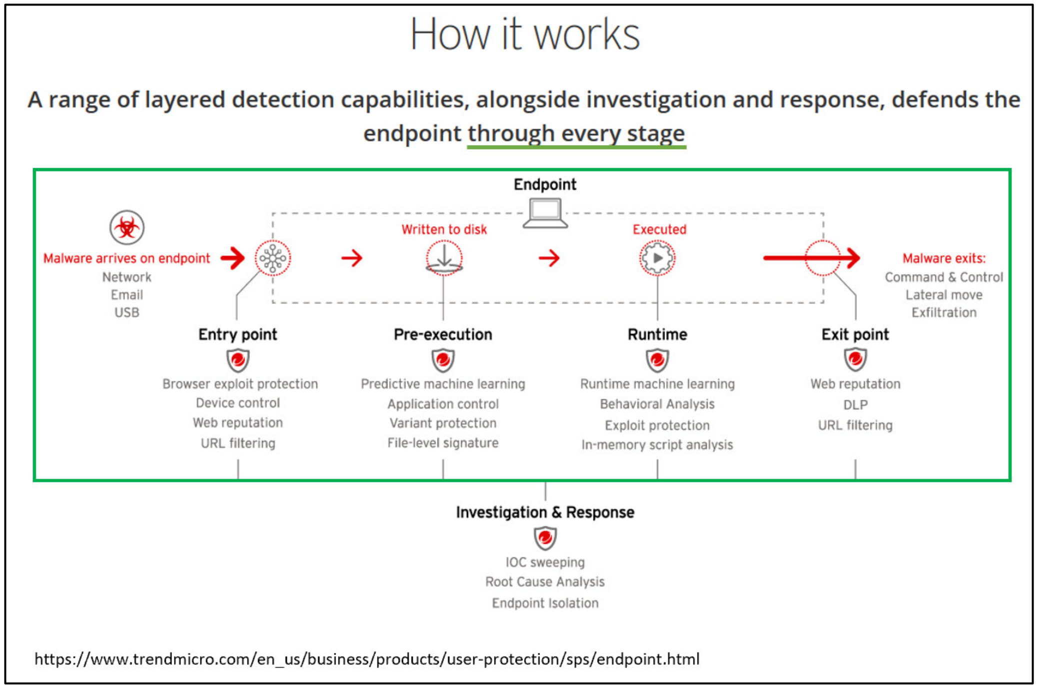
A system and method to securing a computer system from software viruses and other malicious code by intercepting attempts by the malicious code to write data to a storage medium. The invention intercepts the write access requests made by programs and verifies that the program is authorized to write before letting the write proceed. Authorization is determined by using the identity of the program as a query element into a database where permission values are stored. Depending on the presence or value of the permission value, write access is permitted or denied. Permission values can be set by the user, downloaded from a central server, or loaded into the central server by a group of users in order to collectively determine a permission value. The interception code can operate in kernel mode.

11 Claims, 8 Drawing Sheets

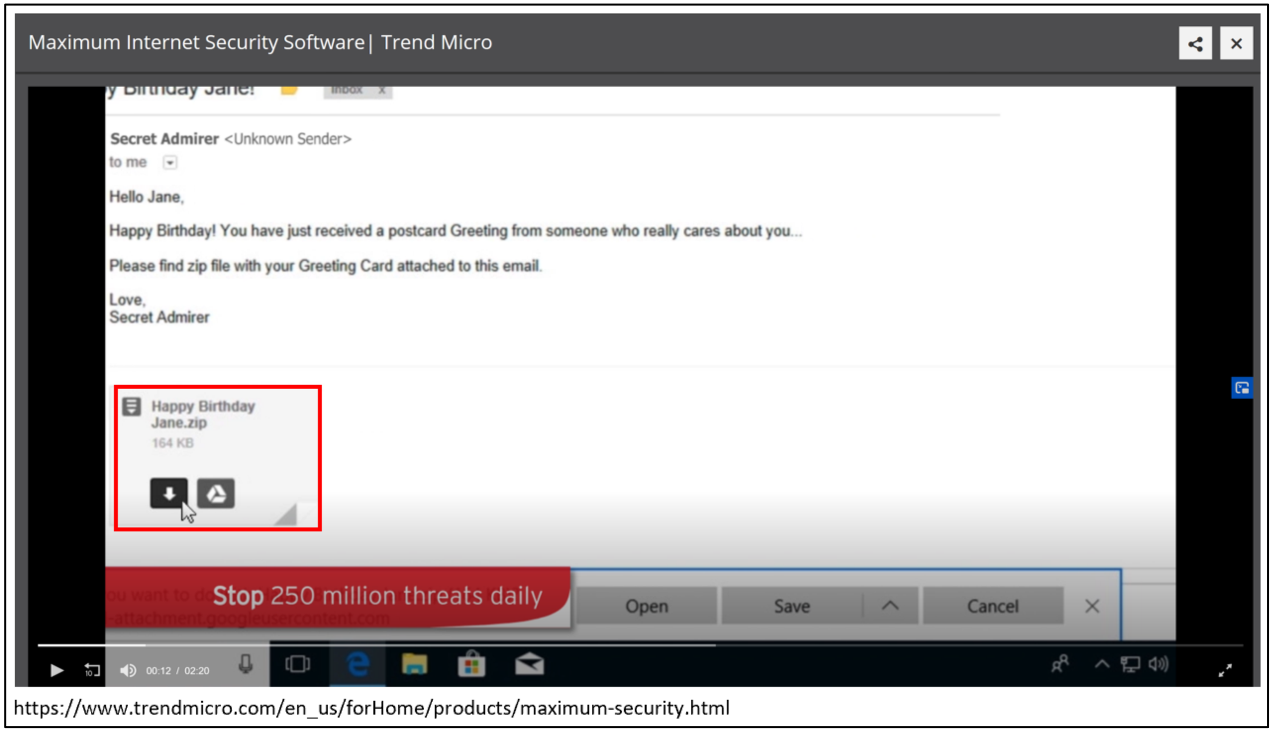
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[pre] In a computer comprising a storage medium and an application running on said computer, a method of controlling write access to said storage medium by said application comprising:	Trend Micro offers various software that performs the method of claim 1. Specifically, Trend Micro offers many applications to protect against electronic threats such as viruses, ransomware, malware, and the like (collectively “hostile applications”). That software includes but is not limited to, OfficeScan, Endpoint Application Control, Apex One, Antivirus+ Security, Internet Security, and Maximum Security. Trend Micro’s software operates and runs on a computer such as a PC, Mac, or Server with a storage medium such as a hard disk or memory. The software controls write access to the computer’s storage medium to prevent hostile applications from writting to the device, which is a central purpose of the software sold by Trend Micro. As illustrated in the graphic below, Trend Micro’s applications allow safe files while blocking malicious files.  LEGEND Known Good Data Known Bad Data Unknown Data Noise Cancellation Web and File Reputation Exploit Prevention Application Control Variant Protection Pre-execution Machine Learning Safe files allowed Behavioral Analysis Runtime Machine Learning Custom Sandbox Analysis Malicious files blocked Investigation & Response Datasheet, Trend Micro Office Scan, at 2

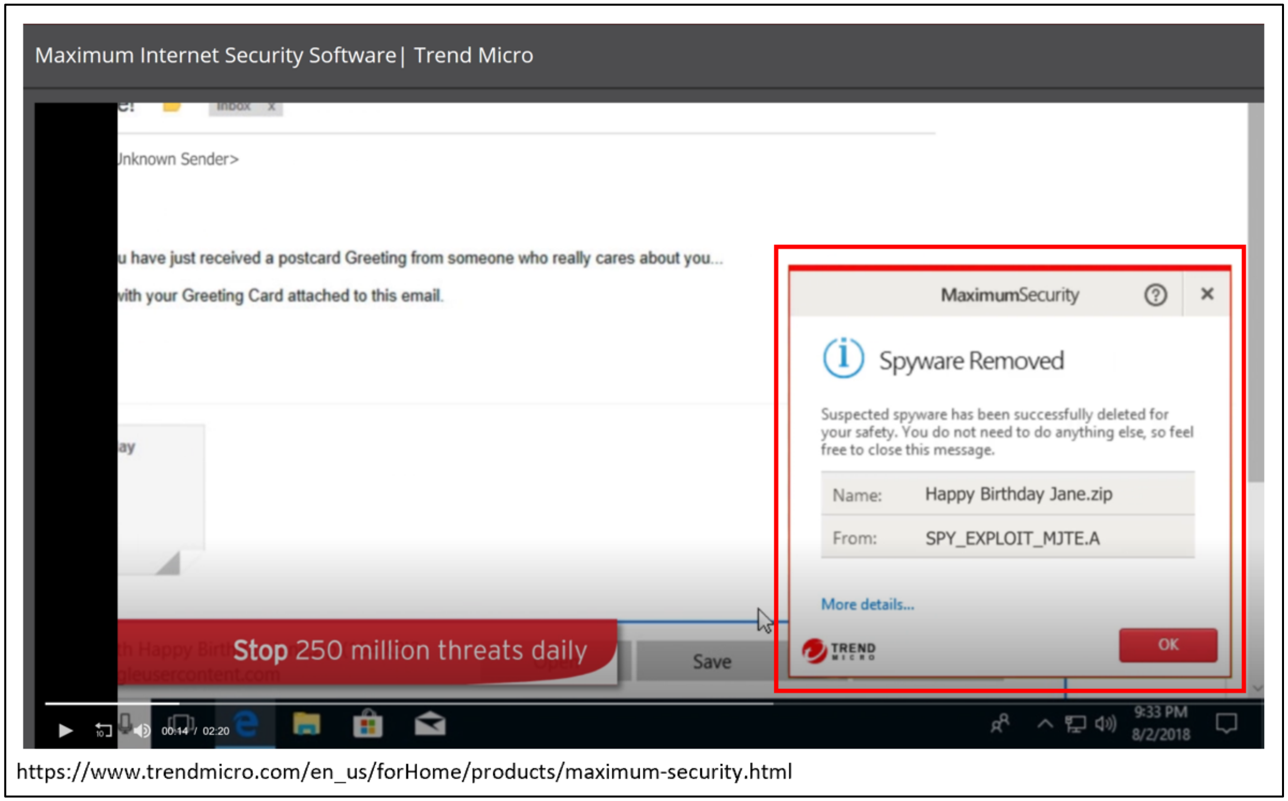
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	Trend Micro's software detects attempts by the application to write data to said storage medium. This attempt to write data can occur during every stage of the hostile application's presence: (1) entry-point; (2) pre-execution; (3) runtime; and (4) exit point. The graphic below showing how Trend Micro's software defends endpoints (e.g., the claimed "computer") is illustrative. First, when a hostile application arrives on an endpoint via for example a network, email, or USB, the software will detect attempts to write. Second, while a hostile application is being written to the storage medium, but before execution, the software detects the attempts to write. Third, while a hostile application is running it can make attempts to write data, which the software will detect. Fourth, when a hostile application exits it can make attempts to write data, which the software will also detect.  How it works A range of layered detection capabilities, alongside investigation and response, defends the endpoint through every stage Endpoint Malware arrives on endpoint Network Email USB Written to disk Executed Malware exits: Command & Control Lateral move Exfiltration Entry point Browser exploit protection Device control Web reputation URL filtering Pre-execution Predictive machine learning Application control Variant protection File-level signature Runtime Runtime machine learning Behavioral Analysis Exploit protection In-memory script analysis Exit point Web reputation DLP URL filtering Investigation & Response IOC sweeping Root Cause Analysis Endpoint Isolation https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html

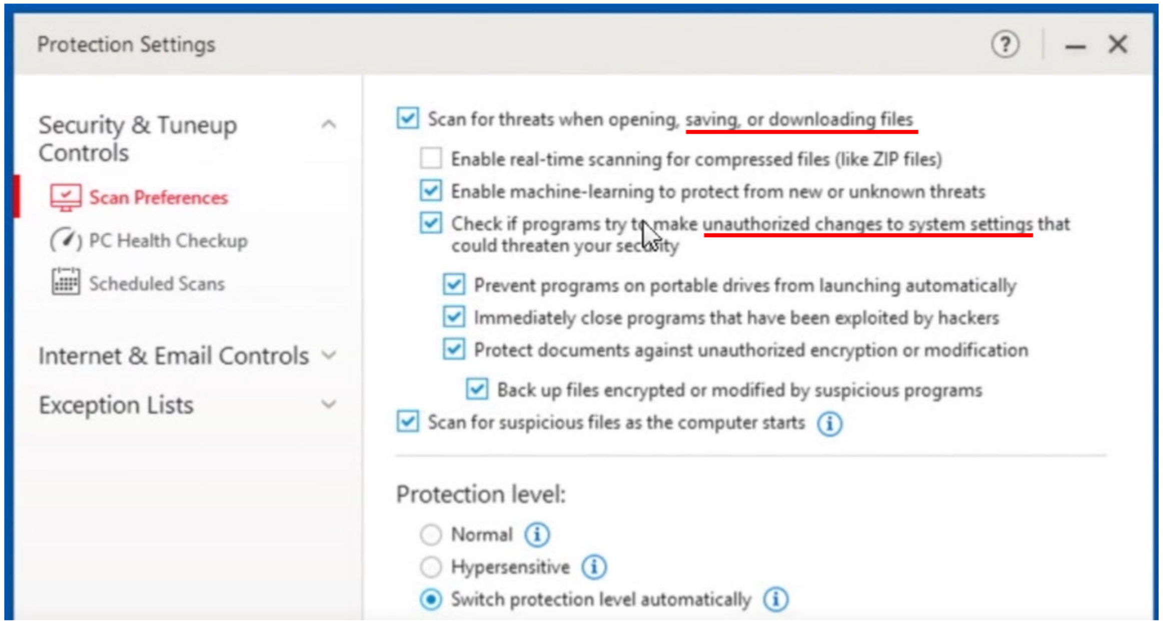
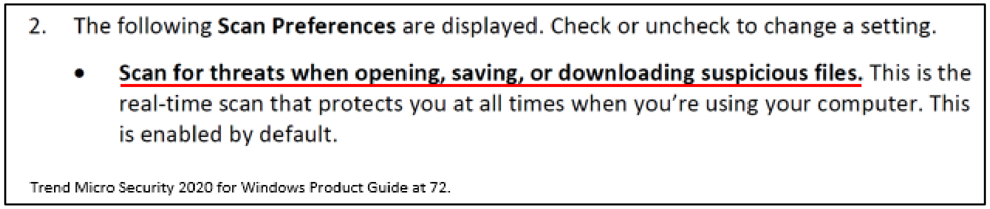
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The remaining slides for limitation 1[a] provide examples of Trend Micro's software detecting attempts by hostile applications to write data to a storage medium in any of the four stages outlined above. The example on this slide shows Trend Micro's Maximum Security detecting an attempt to write by an email attachment. In the image below, the user attempts to and or downloads a zip file from an email attachment, which would cause data to be written to the storage medium. In the image on the next slide, Trend Micro's software detects that attempt to write.  Maximum Internet Security Software | Trend Micro y Birthday Jane! Secret Admirer <Unknown Sender> to me Hello Jane, Happy Birthday! You have just received a postcard Greeting from someone who really cares about you... Please find zip file with your Greeting Card attached to this email. Love, Secret Admirer Happy Birthday Jane.zip 164 KB Inbox x Stop 250 million threats daily Open Save Cancel 00:12 / 02:20 https://www.trendmicro.com/en_us/forHome/products/maximum-security.html

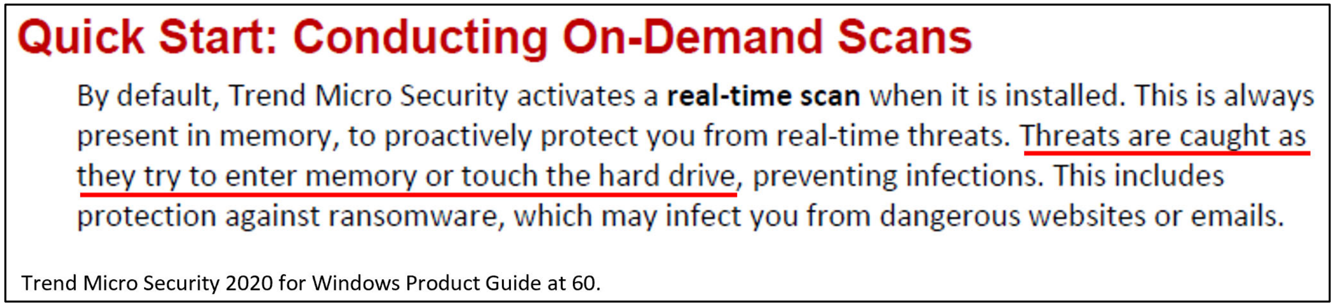
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The image below shows that Trend Micro's software detects that attempt to write before the user has clicked to save the file.  Maximum Internet Security Software| Trend Micro [redacted] e! Inbox x Jnknown Sender> u have just received a postcard Greeting from someone who really cares about you... vith your Greeting Card attached to this email. ay MaximumSecurity Spyware Removed Suspected spyware has been successfully deleted for your safety. You do not need to do anything else, so feel free to close this message. Name: Happy Birthday Jane.zip From: SPY_EXPLOIT_MJTE.A More details... OK Stop 250 million threats daily Save 00:14 / 02:20 9:33 PM 8/2/2018 https://www.trendmicro.com/en_us/forHome/products/maximum-security.html

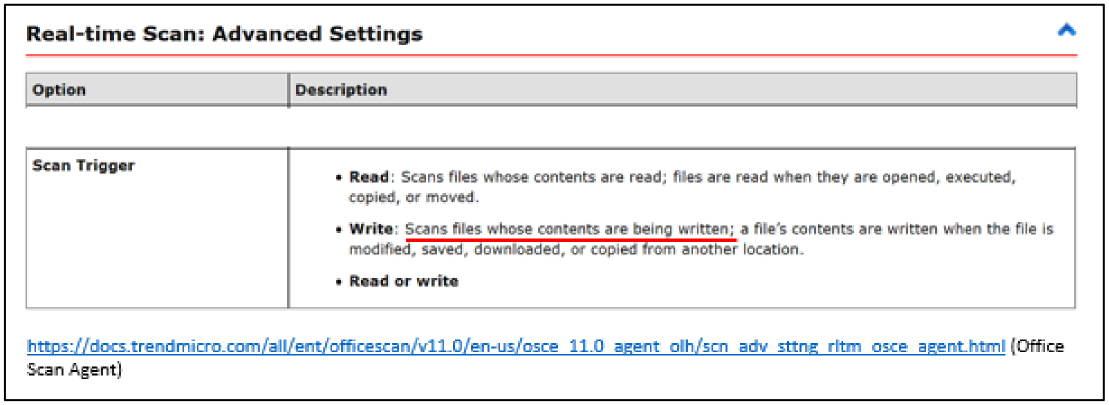
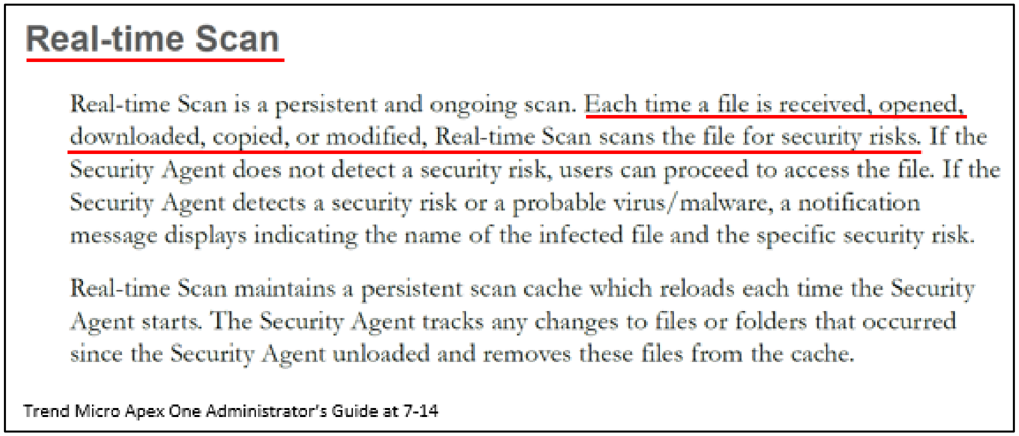
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The image below shows another example of Trend Micro's Security software's ability to detect attempts by hostile applications to write data to a storage medium. As the image shows, the software scans for threats when saving or downloading files or when programs try to make unauthorized changes to system settings.  Protection Settings Security & Tuneup Controls Scan Preferences PC Health Checkup Scheduled Scans Internet & Email Controls Exception Lists ☑ Scan for threats when opening, saving, or downloading files □ Enable real-time scanning for compressed files (like ZIP files) ☑ Enable machine-learning to protect from new or unknown threats ☑ Check if programs try to make unauthorized changes to system settings that could threaten your security ☑ Prevent programs on portable drives from launching automatically ☑ Immediately close programs that have been exploited by hackers ☑ Protect documents against unauthorized encryption or modification ☑ Back up files encrypted or modified by suspicious programs ☑ Scan for suspicious files as the computer starts Protection level: ○ Normal ○ Hypersensitive ● Switch protection level automatically https://www.trendmicro.com/en_us/forHome/products/maximum-security.html  2. The following **Scan Preferences** are displayed. Check or uncheck to change a setting. - Scan for threats when opening, saving, or downloading suspicious files. This is the real-time scan that protects you at all times when you're using your computer. This is enabled by default. Trend Micro Security 2020 for Windows Product Guide at 72.

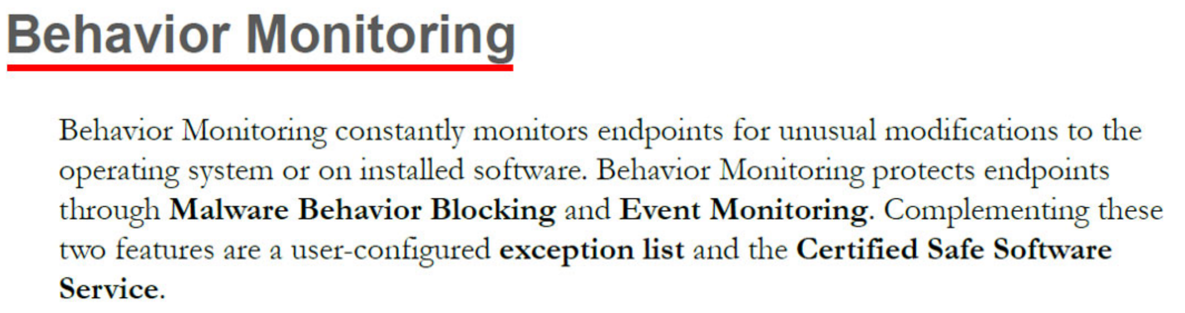
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The image below shows another example of Trend Micro's Security software's ability to detect attempts by hostile applications to write data to a storage medium. As the image shows, threats are caught as they try to enter memory or touch the hard drive.  Quick Start: Conducting On-Demand Scans By default, Trend Micro Security activates a **real-time scan** when it is installed. This is always present in memory, to proactively protect you from real-time threats. Threats are caught as they try to enter memory or touch the hard drive, preventing infections. This includes protection against ransomware, which may infect you from dangerous websites or emails. Trend Micro Security 2020 for Windows Product Guide at 60.

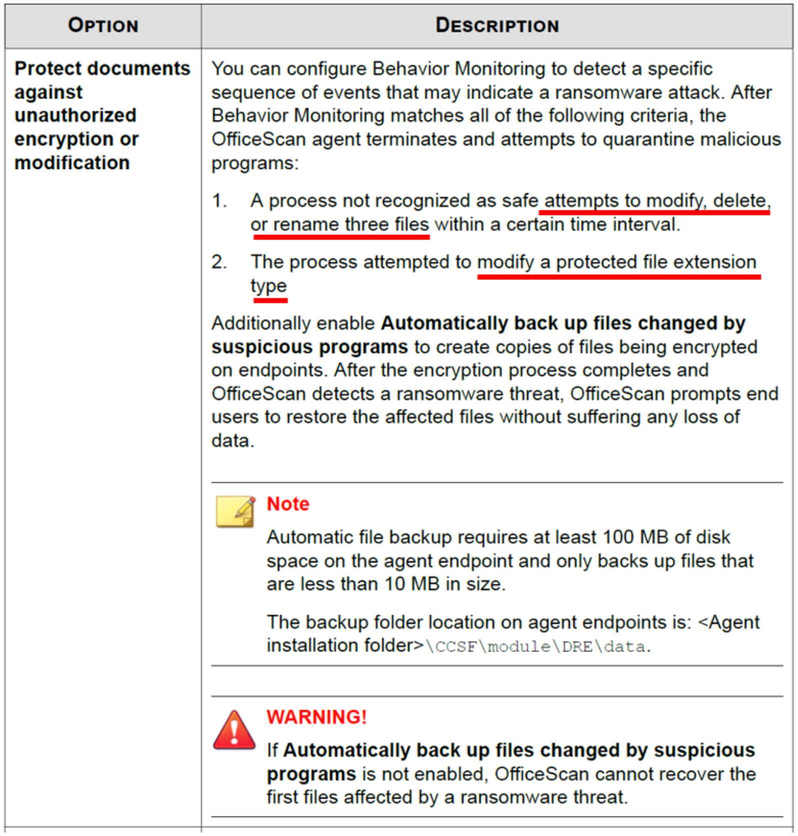
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	Trend Micro's OfficeScan and ApexOne software also include real-time scans, which detect attempts by hostile applications to write data to the computer's storage medium.  **Real-time Scan: Advanced Settings** **Option** — **Description** **Scan Trigger** — • **Read**: Scans files whose contents are read; files are read when they are opened, executed, copied, or moved. • **Write**: Scans files whose contents are being written; a file's contents are written when the file is modified, saved, downloaded, or copied from another location. • **Read or write** https://docs.trendmicro.com/all/ent/officescan/v11.0/en-us/osce_11.0_agent_olh/scn_adv_sttng_rltm_osce_agent.html (Office Scan Agent)  **Real-time Scan** Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If the Security Agent does not detect a security risk, users can proceed to access the file. If the Security Agent detects a security risk or a probable virus/malware, a notification message displays indicating the name of the infected file and the specific security risk. Real-time Scan maintains a persistent scan cache which reloads each time the Security Agent starts. The Security Agent tracks any changes to files or folders that occurred since the Security Agent unloaded and removes these files from the cache. Trend Micro Apex One Administrator's Guide at 7-14

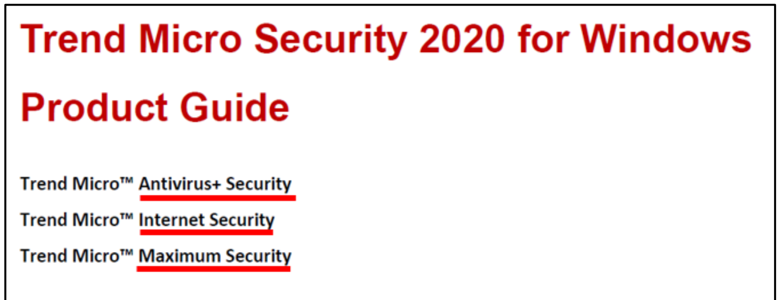
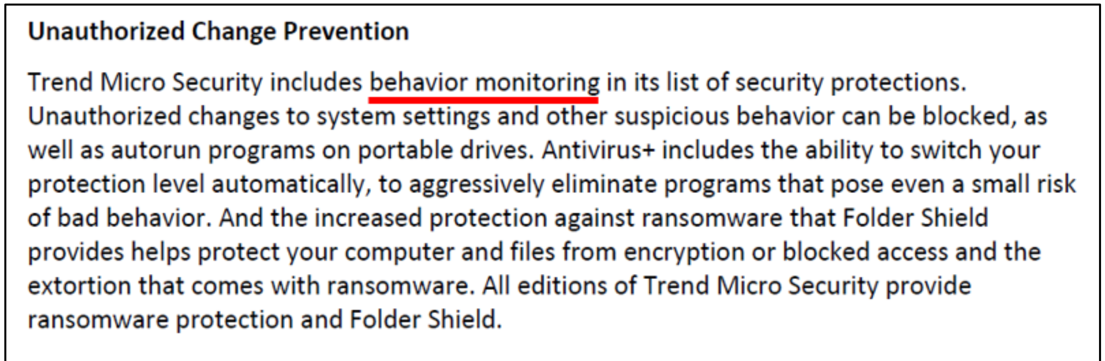
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	Trend Micro's software also includes Behavior Monitoring that detects attempts by hostile applications to write data to the storage medium. As explained in the excerpt below, Behavior Monitoring constantly monitors endpoints, e.g., the claimed computers, for unusual modifications to the operating system or on installed software, e.g., attempts by hostile applications to write data to the storage medium.  **Behavior Monitoring** Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**. Office Scan, Service Pack 1, Administrator's Guide at 9-2

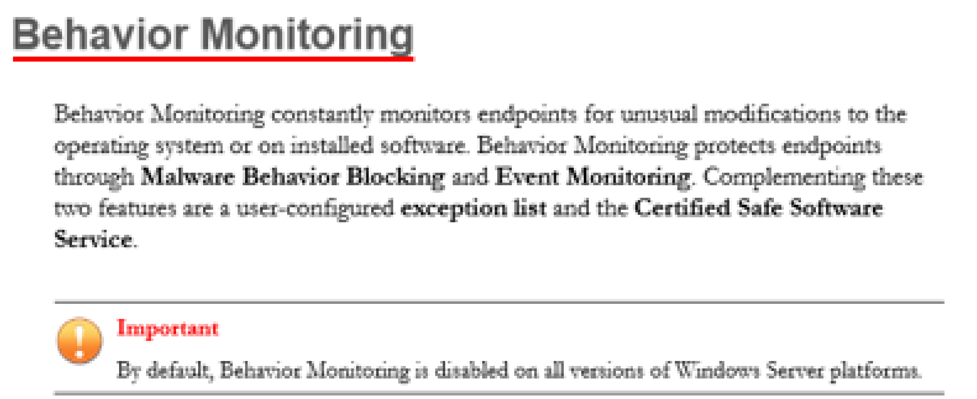
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The Behavior Monitoring service includes ransomware protection that detects attempts by applications to write data to the storage medium of a computer. Those attempts to write occur, for example, in the attempts modify, delete, or rename files or in the modification of the file type.  **OPTION** **DESCRIPTION** **Protect documents against unauthorized encryption or modification** You can configure Behavior Monitoring to detect a specific sequence of events that may indicate a ransomware attack. After Behavior Monitoring matches all of the following criteria, the OfficeScan agent terminates and attempts to quarantine malicious programs: 1. A process not recognized as safe attempts to modify, delete, or rename three files within a certain time interval. 2. The process attempted to modify a protected file extension type Additionally enable **Automatically back up files changed by suspicious programs** to create copies of files being encrypted on endpoints. After the encryption process completes and OfficeScan detects a ransomware threat, OfficeScan prompts end users to restore the affected files without suffering any loss of data. Note Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size. The backup folder location on agent endpoints is: <Agent installation folder>`\CCSF\module\DRE\data`. WARNING! If **Automatically back up files changed by suspicious programs** is not enabled, OfficeScan cannot recover the first files affected by a ransomware threat. Office Scan, Service Pack 1, Administrator's Guide at 9-4

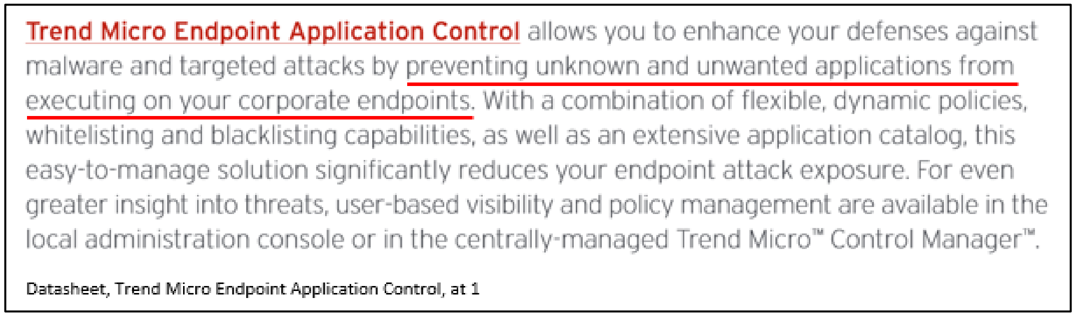
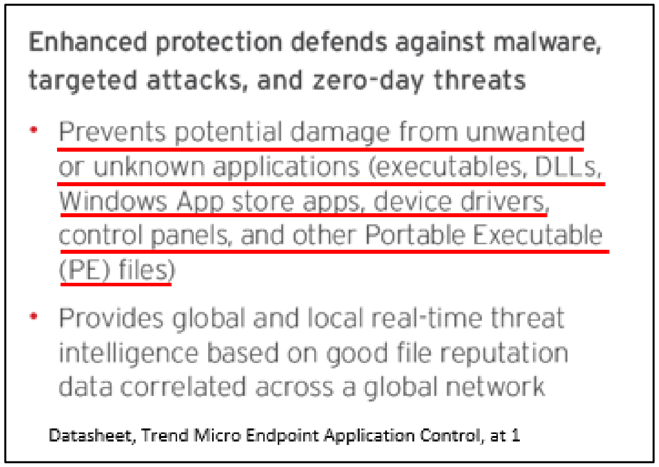
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The following excerpt shows that Trend Micro's Security software (Antivirus+ Security, Internet Security, and Maximum Security) also include Behavior Monitoring functionality.  **Trend Micro Security 2020 for Windows Product Guide** Trend Micro™ Antivirus+ Security Trend Micro™ Internet Security Trend Micro™ Maximum Security Trend Micro Security 2020 for Windows Product Guide at 1.  **Unauthorized Change Prevention** Trend Micro Security includes behavior monitoring in its list of security protections. Unauthorized changes to system settings and other suspicious behavior can be blocked, as well as autorun programs on portable drives. Antivirus+ includes the ability to switch your protection level automatically, to aggressively eliminate programs that pose even a small risk of bad behavior. And the increased protection against ransomware that Folder Shield provides helps protect your computer and files from encryption or blocked access and the extortion that comes with ransomware. All editions of Trend Micro Security provide ransomware protection and Folder Shield. Trend Micro Security 2020 for Windows Product Guide at 70.

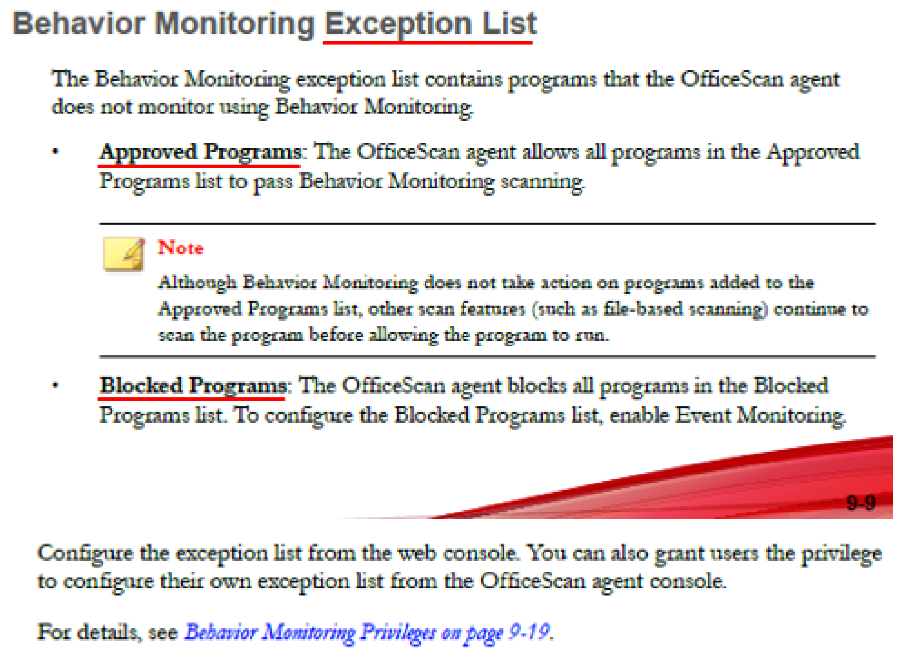
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	The following excerpt shows that Apex One also includes Behavior Monitoring functionality.  **Behavior Monitoring** Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**. **Important** By default, Behavior Monitoring is disabled on all versions of Windows Server platforms. Trend Micro Apex One Administrator's Guide at 9-2

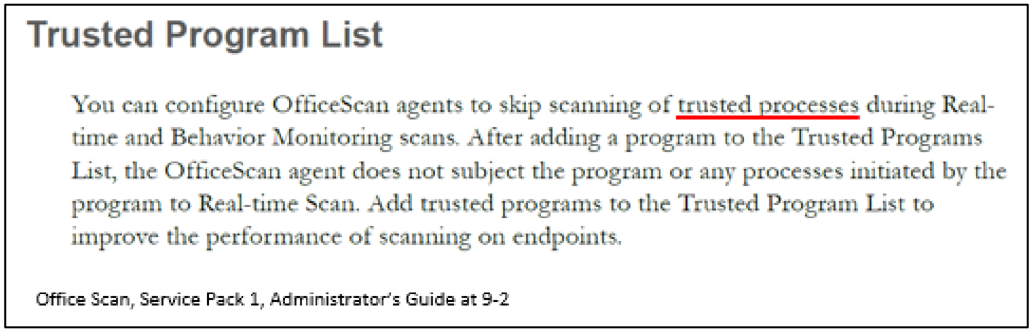
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

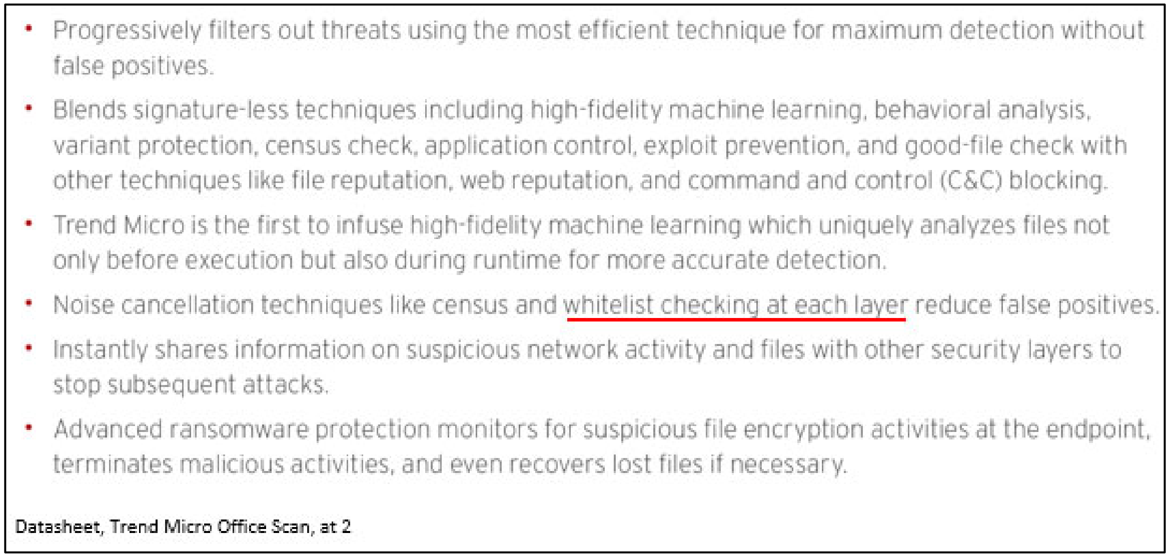
CLAIM 1	TREND MICRO PRODUCTS
1[a] detecting an attempt by the application to write data to said storage medium;	Trend Micro's Endpoint Application Control software also detects attempts by hostile applications to write data to a computer's storage medium. Endpoint Application Control detects those attempt to prevent them from occurring. For example it detects write attempts by executables, DDLs, Windows App store apps, device drivers, controls panels, and other portable executable files.  Trend Micro Endpoint Application Control allows you to enhance your defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on your corporate endpoints. With a combination of flexible, dynamic policies, whitelisting and blacklisting capabilities, as well as an extensive application catalog, this easy-to-manage solution significantly reduces your endpoint attack exposure. For even greater insight into threats, user-based visibility and policy management are available in the local administration console or in the centrally-managed Trend Micro™ Control Manager™. Datasheet, Trend Micro Endpoint Application Control, at 1  **Enhanced protection defends against malware, targeted attacks, and zero-day threats** • Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files) • Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network Datasheet, Trend Micro Endpoint Application Control, at 1

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

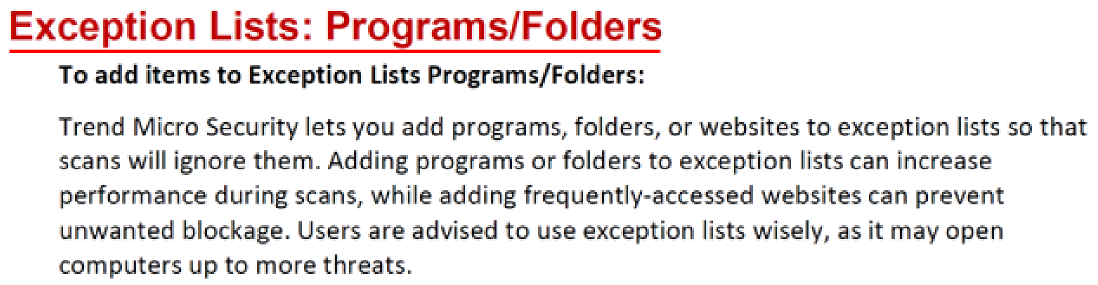
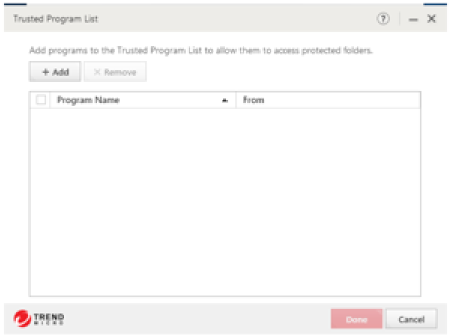
CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	In response to the write attempts discussed for limitation 1[a], OfficeScan attempts to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications. For example, the Behavior Monitoring functionality includes an exception list for approved programs and blocked programs. If a program is on the exception list as an approved program, Office Scan does not monitor that program. If a program is on the exception list as a blocked program, Office Scan blocks that program. Upon information and belief, the programs on the exception list are stored on a database that include data elements encoding permission values, e.g., approved or blocked, that are associated with the applications on the list.  **Behavior Monitoring Exception List** The Behavior Monitoring exception list contains programs that the OfficeScan agent does not monitor using Behavior Monitoring. • **Approved Programs**: The OfficeScan agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning. Note Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run. • **Blocked Programs**: The OfficeScan agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring. 9-9 Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the OfficeScan agent console. For details, see *Behavior Monitoring Privileges on page 9-19*. Office Scan, Service Pack 1, Administrator's Guide at 9-9, 10.

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

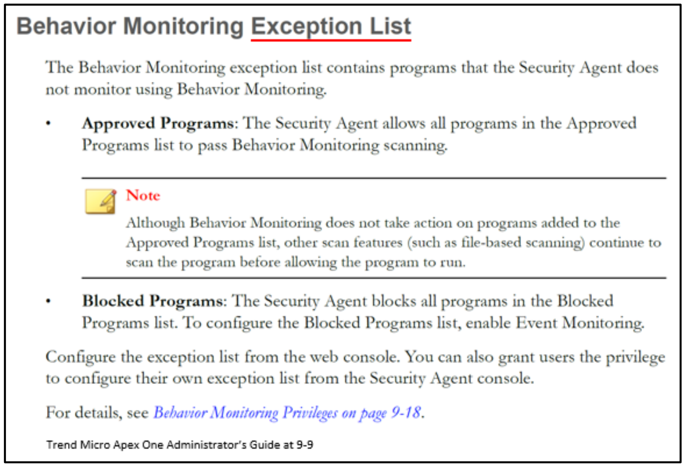
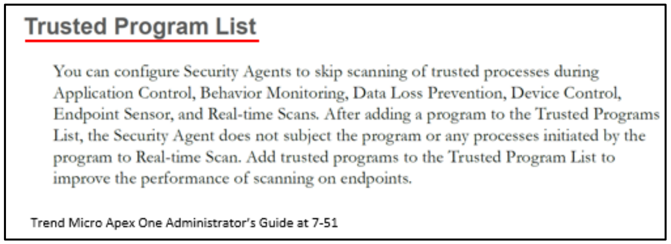
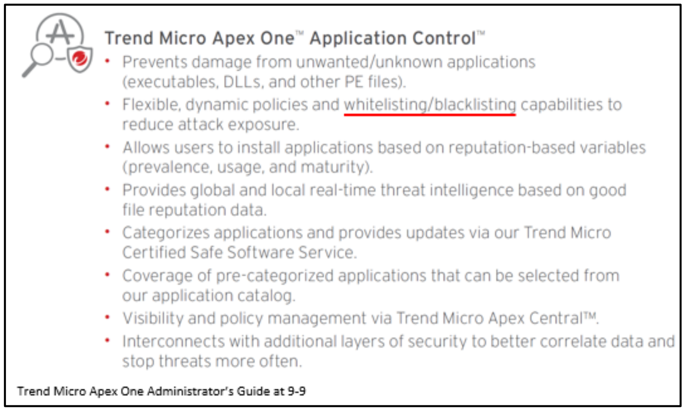
CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	The Office Scan software also includes a Trusted Program list. Upon information and belief, the programs on that list are stored on a database that include data elements encoding permission values, e.g., trusted or not, that are associated with the applications on the list.  **Trusted Program List** You can configure OfficeScan agents to skip scanning of trusted processes during Real-time and Behavior Monitoring scans. After adding a program to the Trusted Programs List, the OfficeScan agent does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints. Office Scan, Service Pack 1, Administrator's Guide at 9-2

CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	Office Scan performs whitelist checking such as the exception list and trusted programs lists at each layer, i.e., at each the stages discussed on slide 3.  • Progressively filters out threats using the most efficient technique for maximum detection without false positives. • Blends signature-less techniques including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking. • Trend Micro is the first to infuse high-fidelity machine learning which uniquely analyzes files not only before execution but also during runtime for more accurate detection. • Noise cancellation techniques like census and whitelist checking at each layer reduce false positives. • Instantly shares information on suspicious network activity and files with other security layers to stop subsequent attacks. • Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, terminates malicious activities, and even recovers lost files if necessary. Datasheet, Trend Micro Office Scan, at 2

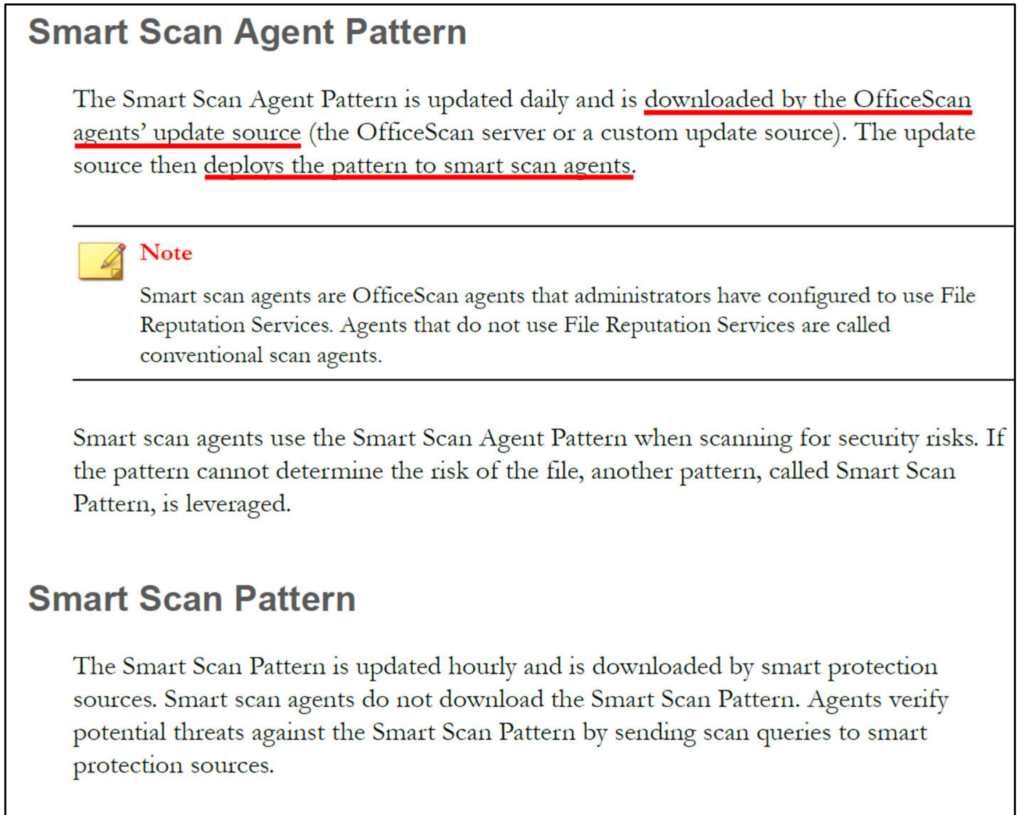
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	Trend Micro's other software packages also include exception lists and trusted programs list. The following excerpt shows that Antivirus+ Security, Internet Security, and Maximum Security also include exception lists / trusted program lists.  **Exception Lists: Programs/Folders** **To add items to Exception Lists Programs/Folders:** Trend Micro Security lets you add programs, folders, or websites to exception lists so that scans will ignore them. Adding programs or folders to exception lists can increase performance during scans, while adding frequently-accessed websites can prevent unwanted blockage. Users are advised to use exception lists wisely, as it may open computers up to more threats. Trend Micro Security 2020 for Windows Product Guide at 84. 13. You can also click the link **Trusted Program List** to add a trusted program to a list of applications that can access protected folders. The **Trusted Program List** appears.  Trusted Program List Add programs to the Trusted Program List to allow them to access protected folders. + Add × Remove Program Name From TREND MICRO Done Cancel **Figure 193. Trusted Program List** Trend Micro Security 2020 for Windows Product Guide at 110-111.

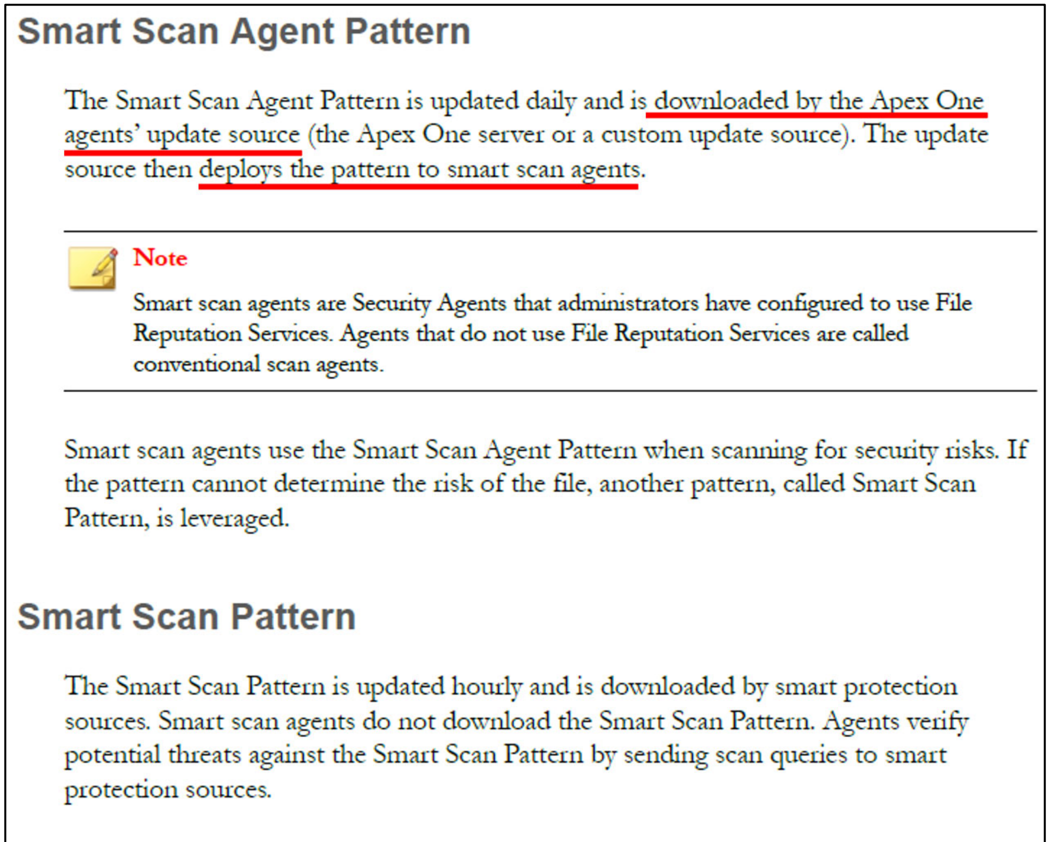
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	The following excerpts also show that Apex One includes exception lists and trusted program lists.  **Behavior Monitoring Exception List** The Behavior Monitoring exception list contains programs that the Security Agent does not monitor using Behavior Monitoring. - **Approved Programs**: The Security Agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning. Note Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run. - **Blocked Programs**: The Security Agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring. Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the Security Agent console. For details, see *Behavior Monitoring Privileges on page 9-18*. Trend Micro Apex One Administrator's Guide at 9-9  **Trusted Program List** You can configure Security Agents to skip scanning of trusted processes during Application Control, Behavior Monitoring, Data Loss Prevention, Device Control, Endpoint Sensor, and Real-time Scans. After adding a program to the Trusted Programs List, the Security Agent does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints. Trend Micro Apex One Administrator's Guide at 7-51  Trend Micro Apex One™ Application Control™ - Prevents damage from unwanted/unknown applications (executables, DLLs, and other PE files). - Flexible, dynamic policies and whitelisting/blacklisting capabilities to reduce attack exposure. - Allows users to install applications based on reputation-based variables (prevalence, usage, and maturity). - Provides global and local real-time threat intelligence based on good file reputation data. - Categorizes applications and provides updates via our Trend Micro Certified Safe Software Service. - Coverage of pre-categorized applications that can be selected from our application catalog. - Visibility and policy management via Trend Micro Apex Central™. - Interconnects with additional layers of security to better correlate data and stop threats more often. Trend Micro Apex One Administrator's Guide at 9-9

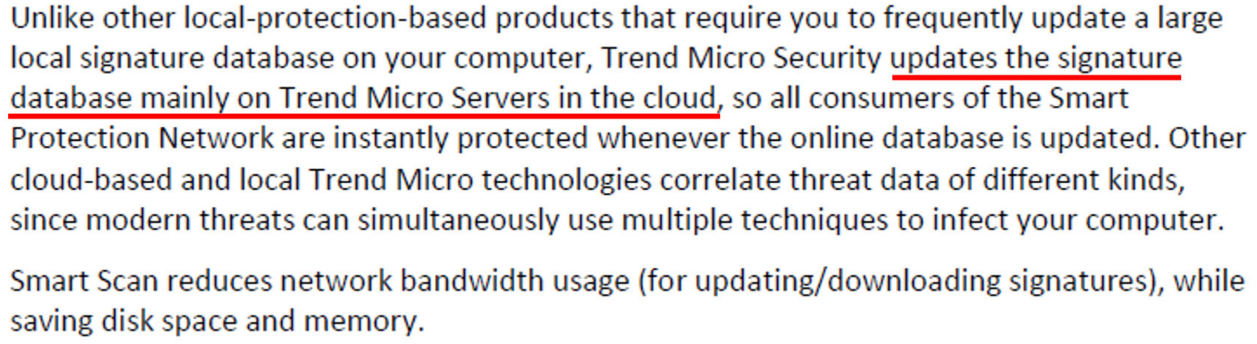
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	The following excerpts also show that, during for example real-time scans discussed above, Office Scan and Apex One attempt to retrieve permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications. Those permission values are stored on a database containing the Smart Scan Agent Pattern on the computer.  **Smart Scan Agent Pattern** The Smart Scan Agent Pattern is updated daily and is downloaded by the OfficeScan agents' update source (the OfficeScan server or a custom update source). The update source then deploys the pattern to smart scan agents. **Note** Smart scan agents are OfficeScan agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents. Smart scan agents use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged. **Smart Scan Pattern** The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan agents do not download the Smart Scan Pattern. Agents verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources. Office Scan, Service Pack 1, Administrator's Guide at 4-8

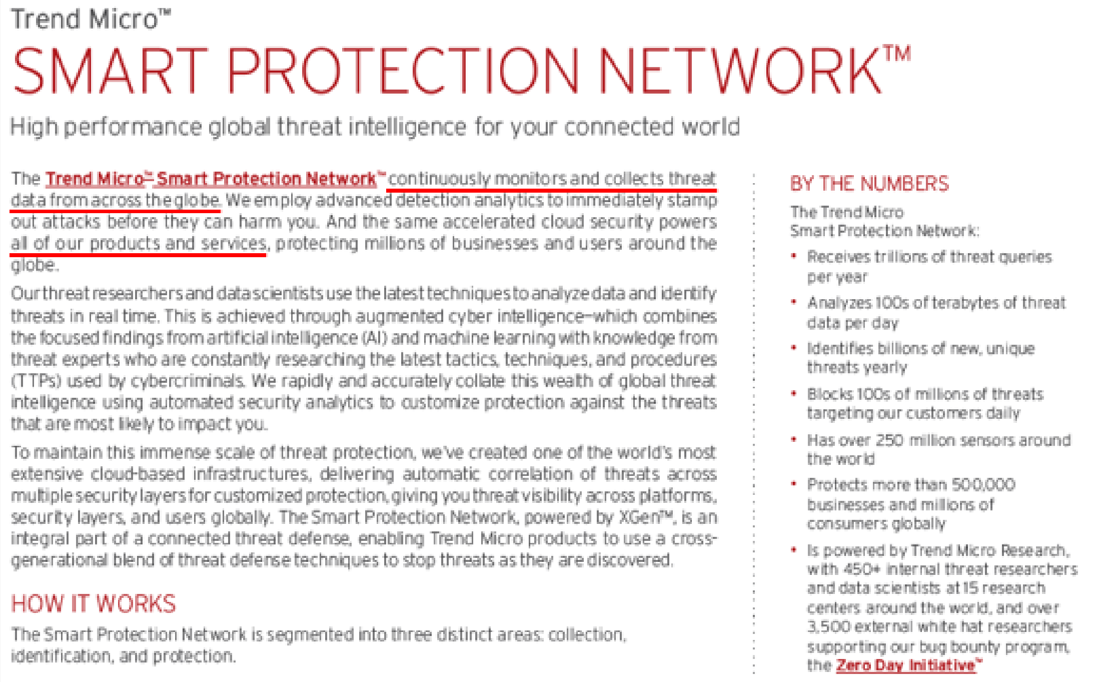
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	The following excerpts shows the same Smart Scan Agent Pattern for the Apex One.  **Smart Scan Agent Pattern** The Smart Scan Agent Pattern is updated daily and is downloaded by the Apex One agents' update source (the Apex One server or a custom update source). The update source then deploys the pattern to smart scan agents. Note Smart scan agents are Security Agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents. Smart scan agents use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged. **Smart Scan Pattern** The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan agents do not download the Smart Scan Pattern. Agents verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources. Trend Micro Apex One Administrator's Guide at 4-8

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[b] in response to said write attempt, attempting to retrieve a permission value from a database comprised of data elements encoding at least one permission value associated with one or more applications;	Trend Micro's Security software also uses a local database of permission values in combination with the online database of the Smart Protection Network. The signature database is maintained "mainly on Trend Micro Servers in the cloud," which means that at least some of the database is stored locally.  Unlike other local-protection-based products that require you to frequently update a large local signature database on your computer, Trend Micro Security updates the signature database mainly on Trend Micro Servers in the cloud, so all consumers of the Smart Protection Network are instantly protected whenever the online database is updated. Other cloud-based and local Trend Micro technologies correlate threat data of different kinds, since modern threats can simultaneously use multiple techniques to infect your computer. Smart Scan reduces network bandwidth usage (for updating/downloading signatures), while saving disk space and memory. Trend Micro Security 2020 for Windows Product Guide at 61.

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;	In the case where no permission value for the running application is found in the database, e.g., no exception list, trusted list entry, or pattern detection, Trend Micro transmits a query comprised of an indicia of identity associated with said running application to a central server operatively connected to the computer and to at least one additional computer. For example, this step occurs via Trend Micro's Smart Protection Network. Trend Micro's Smart Protection Network servers continually monitor and collect threat data from across the globe. All Trend Micro products and services use the Smart Protection Network. Thus, all computers running Trend Micro's software are connected to the Smart Protection Network servers.  Trend Micro™ SMART PROTECTION NETWORK™ High performance global threat intelligence for your connected world The Trend Micro™ Smart Protection Network™ continuously monitors and collects threat data from across the globe. We employ advanced detection analytics to immediately stamp out attacks before they can harm you. And the same accelerated cloud security powers all of our products and services, protecting millions of businesses and users around the globe. Our threat researchers and data scientists use the latest techniques to analyze data and identify threats in real time. This is achieved through augmented cyber intelligence–which combines the focused findings from artificial intelligence (AI) and machine learning with knowledge from threat experts who are constantly researching the latest tactics, techniques, and procedures (TTPs) used by cybercriminals. We rapidly and accurately collate this wealth of global threat intelligence using automated security analytics to customize protection against the threats that are most likely to impact you. To maintain this immense scale of threat protection, we've created one of the world's most extensive cloud-based infrastructures, delivering automatic correlation of threats across multiple security layers for customized protection, giving you threat visibility across platforms, security layers, and users globally. The Smart Protection Network, powered by XGen™, is an integral part of a connected threat defense, enabling Trend Micro products to use a cross-generational blend of threat defense techniques to stop threats as they are discovered. HOW IT WORKS The Smart Protection Network is segmented into three distinct areas: collection, identification, and protection. BY THE NUMBERS The Trend Micro Smart Protection Network: • Receives trillions of threat queries per year • Analyzes 100s of terabytes of threat data per day • Identifies billions of new, unique threats yearly • Blocks 100s of millions of threats targeting our customers daily • Has over 250 million sensors around the world • Protects more than 500,000 businesses and millions of consumers globally • Is powered by Trend Micro Research, with 450+ internal threat researchers and data scientists at 15 research centers around the world, and over 3,500 external white hat researchers supporting our bug bounty program, the Zero Day Initiative™ Datasheet, Trend Micro Smart Protection Network, at 1

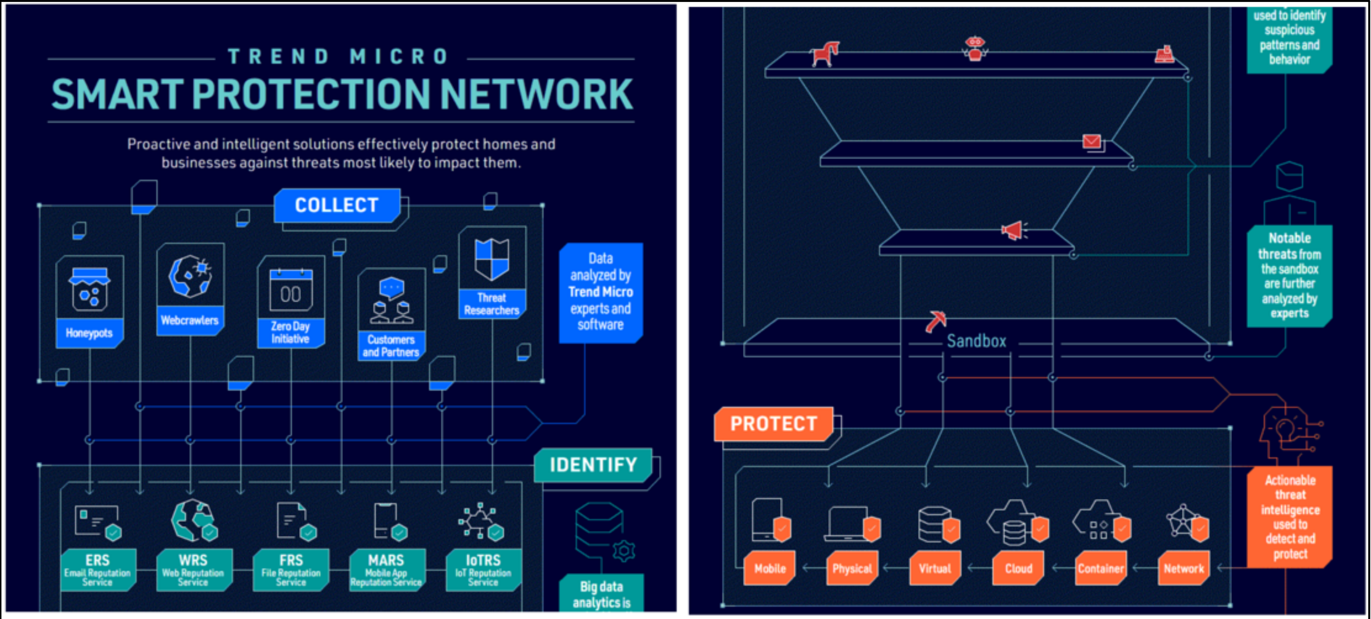
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

<table>
<tr><th>CLAIM 1</th><th>TREND MICRO PRODUCTS</th></tr>
<tr><td>

1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;

</td><td>

Trend Micro's Smart Protection Network servers are connected to at least one additional computer. Those additional computers include for example honeypots, webcrawlers, zero day initiatives, customers and partners, threat researchers, and the sandbox.

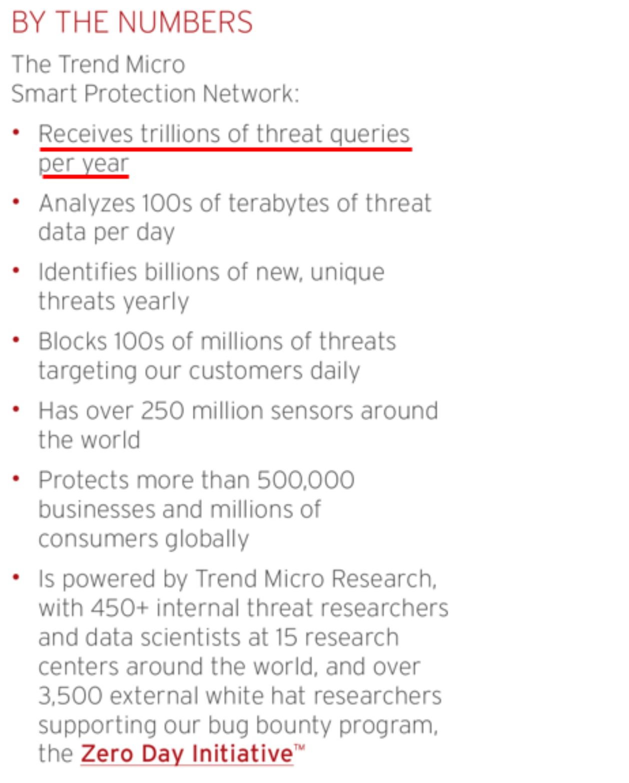


TREND MICRO
SMART PROTECTION NETWORK
Proactive and intelligent solutions effectively protect homes and businesses against threats most likely to impact them.
COLLECT
Honeypots
Webcrawlers
Zero Day Initiative
Customers and Partners
Threat Researchers
Data analyzed by Trend Micro experts and software
IDENTIFY
ERS Email Reputation Service
WRS Web Reputation Service
FRS File Reputation Service
MARS Mobile App Reputation Service
IoTRS IoT Reputation Service
Big data analytics is
used to identify suspicious patterns and behavior
Notable threats from the sandbox are further analyzed by experts
Sandbox
PROTECT
Mobile
Physical
Virtual
Cloud
Container
Network
Actionable threat intelligence used to detect and protect

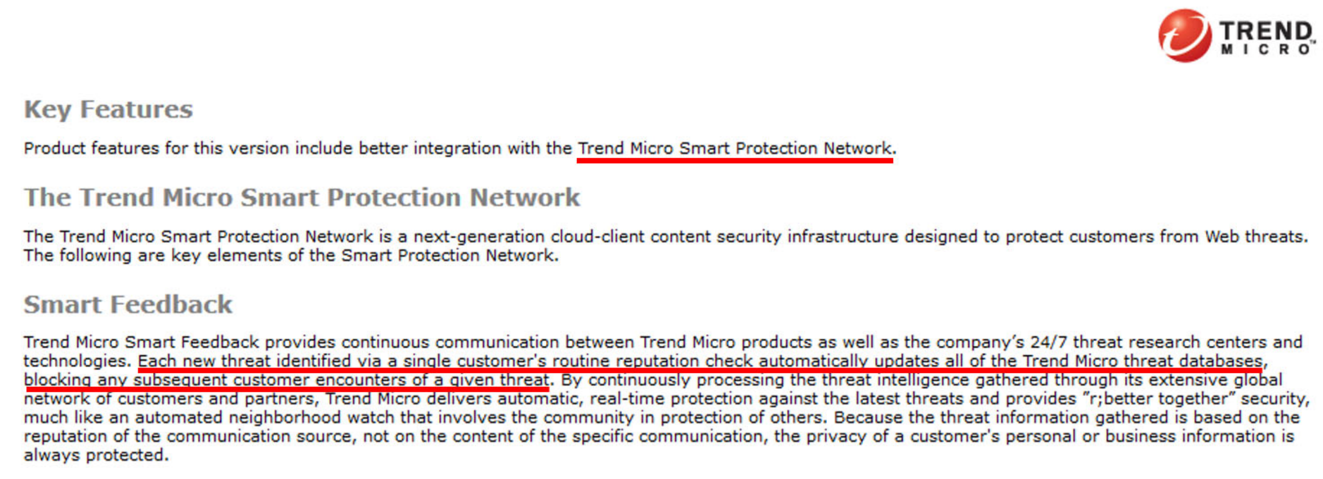
https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html

</td></tr>
</table>

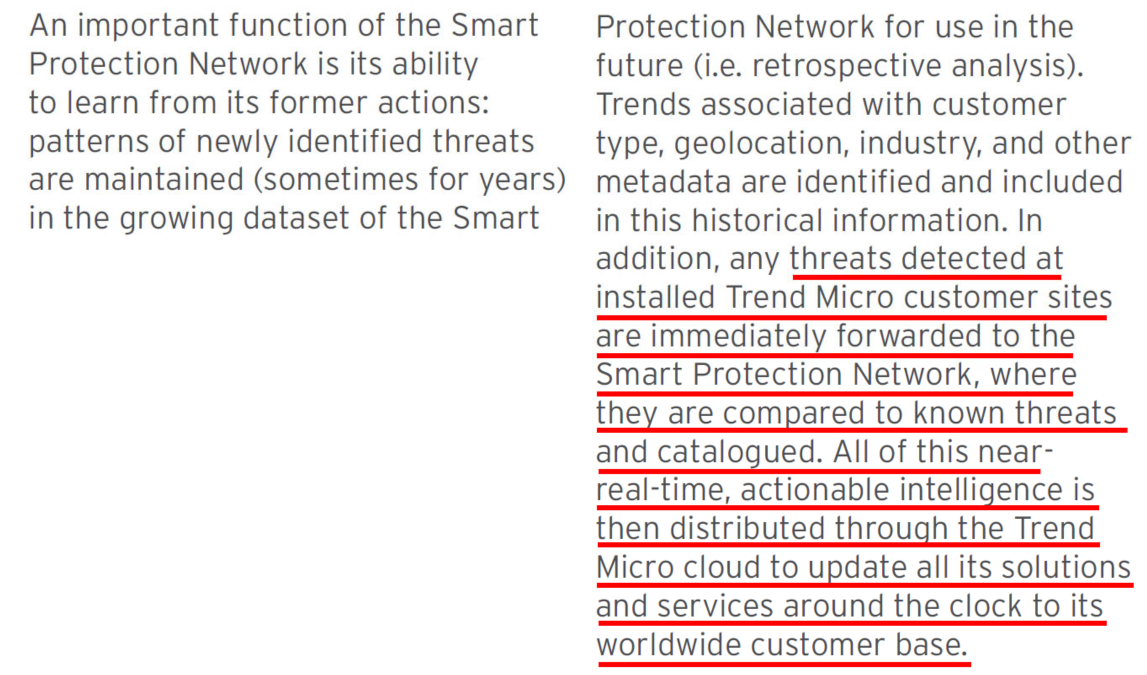
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[c] in the case that no permission value for the running application is found in the database, transmitting to a central server operatively connected to the computer and to at least one additional computer, a query comprised of an indicia of identity associated with said running application;	The computer using Trend Micro's software transmits a query to Trend Micro's Smart Protection Network comprised of an indicia of identity associated with said running application. As noted below, the Smart Protection Network receives trillions of threat queries per year. For the Smart Protection Network to identify the suspected threat and respond to the query, the query must include an indicia of identity associated with the running application.  BY THE NUMBERS The Trend Micro Smart Protection Network: • Receives trillions of threat queries per year • Analyzes 100s of terabytes of threat data per day • Identifies billions of new, unique threats yearly • Blocks 100s of millions of threats targeting our customers daily • Has over 250 million sensors around the world • Protects more than 500,000 businesses and millions of consumers globally • Is powered by Trend Micro Research, with 450+ internal threat researchers and data scientists at 15 research centers around the world, and over 3,500 external white hat researchers supporting our bug bounty program, the **Zero Day Initiative**™ Datasheet, Trend Micro Smart Protection Network, at 1

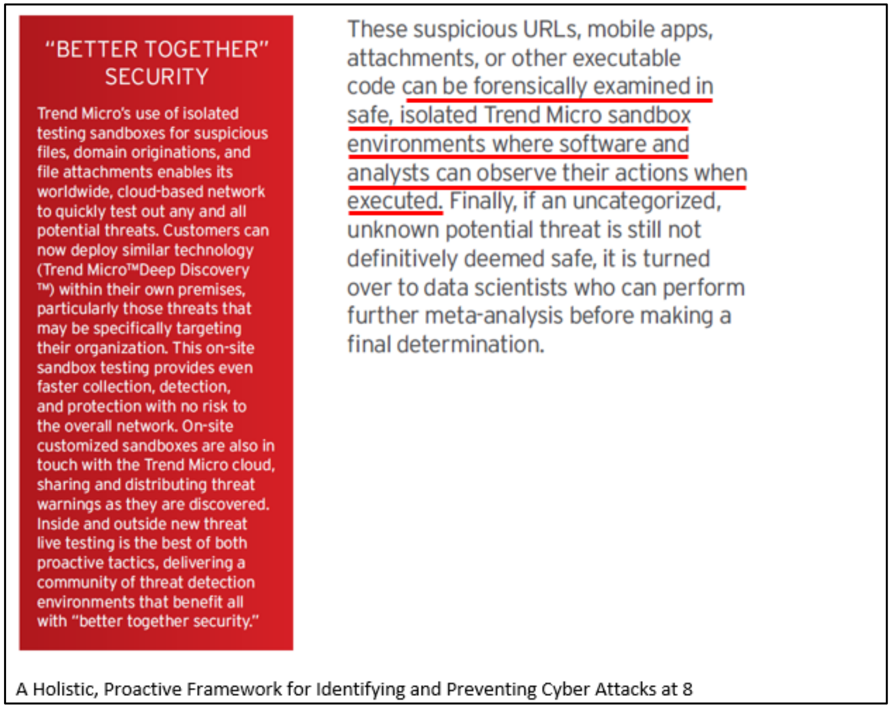
Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.	The computer running Trend Micro's software receives from said central servers of the Smart Protection Network, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer. For example, Trend Micro's customers and partners provide smart feedback to the Smart Protection Network. Once a threat is identified via that feedback, Trend Micro updates the Smart Protection Network to block any subsequent encounters of that threat by any other Trend Micro customers or partners. Thus, the claimed computer receives from the central servers of the Smart Protection network data that represents the collective response to block the requests of the hostile application by all computers after the original encounter that identified the threat.  Key Features Product features for this version include better integration with the Trend Micro Smart Protection Network. The Trend Micro Smart Protection Network The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from Web threats. The following are key elements of the Smart Protection Network. Smart Feedback Trend Micro Smart Feedback provides continuous communication between Trend Micro products as well as the company's 24/7 threat research centers and technologies. Each new threat identified via a single customer's routine reputation check automatically updates all of the Trend Micro threat databases, blocking any subsequent customer encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "r;better together" security, much like an automated neighborhood watch that involves the community in protection of others. Because the threat information gathered is based on the reputation of the communication source, not on the content of the specific communication, the privacy of a customer's personal or business information is always protected. https://docs.trendmicro.com/all/smb/wfbs-a/v7.0/en-us/wfbs-a_7.0_olh/WFBS/Introducing_WFBS/KeyFeatures.htm

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.	The image below further shows that the claimed computer receives from the central servers of the Smart Protection network data that represents the collective response to block the requests of the hostile application by all computers after the original encounter that identified the threat. Alternatively, if the application is benign, the Smart Protection Network sends a corresponding response that is representative of other responses from users that have similarly allowed access and been unharmed.  An important function of the Smart Protection Network is its ability to learn from its former actions: patterns of newly identified threats are maintained (sometimes for years) in the growing dataset of the Smart Protection Network for use in the future (i.e. retrospective analysis). Trends associated with customer type, geolocation, industry, and other metadata are identified and included in this historical information. In addition, any threats detected at installed Trend Micro customer sites are immediately forwarded to the Smart Protection Network, where they are compared to known threats and catalogued. All of this near-real-time, actionable intelligence is then distributed through the Trend Micro cloud to update all its solutions and services around the clock to its worldwide customer base. A Holistic, Proactive Framework for Identifying and Preventing Cyber Attacks at 8

Ex. D – Claim Chart
U.S. Patent No. 7,664,924

CLAIM 1	TREND MICRO PRODUCTS
1[d] receiving from said central server, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer.	The computer running Trend Micro's software receives from said central servers of the Smart Protection Network, data that represents the collective response of the user of the at least one additional computer to requests by the same application running on said at least one additional computer to access the storage medium that comprises said at least one additional computer. For example, the additional computers in the sandbox allow the requests by the application to access their storage mediums, and if found harmless, the Smart Protection Network sends data to the computer indicating that the requests by the application should be allowed.  "BETTER TOGETHER" SECURITY Trend Micro's use of isolated testing sandboxes for suspicious files, domain originations, and file attachments enables its worldwide, cloud-based network to quickly test out any and all potential threats. Customers can now deploy similar technology (Trend Micro™Deep Discovery ™) within their own premises, particularly those threats that may be specifically targeting their organization. This on-site sandbox testing provides even faster collection, detection, and protection with no risk to the overall network. On-site customized sandboxes are also in touch with the Trend Micro cloud, sharing and distributing threat warnings as they are discovered. Inside and outside new threat live testing is the best of both proactive tactics, delivering a community of threat detection environments that benefit all with "better together security." These suspicious URLs, mobile apps, attachments, or other executable code can be forensically examined in safe, isolated Trend Micro sandbox environments where software and analysts can observe their actions when executed. Finally, if an uncategorized, unknown potential threat is still not definitively deemed safe, it is turned over to data scientists who can perform further meta-analysis before making a final determination. A Holistic, Proactive Framework for Identifying and Preventing Cyber Attacks at 8